Fact Sheet: DOE Award Selections for the Research, Development, and Demonstration of Next-Generation Cybersecurity Tools and Technologies for Critical Energy Infrastructure

On October 1, 2018, the Department of Energy (DOE) announced the award of up to $28 million to support the research, development, and demonstration (RD&D) of next-generation tools and technologies that will improve the cybersecurity and resilience of the Nation's energy critical infrastructure, including the electric grid and oil and natural gas infrastructure.

Selected projects will promote industry's advancement of technologies in five important areas:

- Redesign for Cyber-resilient Architecture – Electric and Oil and Natural Gas (ONG) Subsectors
- Cybersecurity for the ONG Environment
- Cybersecure Communications
- Cybersecure Cloud-based Technologies in the Operation Technology (OT) Environment
- Innovative Technologies that Enhance Cybersecurity in the Energy Sector

Below are details about the award recipients and the projects.

Project Performer	Project Partners	Project Title	Project Description
ABB, Inc.	• Iowa State University • University of Illinois Urbana-Champaign	Cyber Resilient Flexible AC Transmission Systems (FACTS)	The project team will leverage power grid physics, computer science, and power engineering principles to develop methods and defense-in-depth cybersecurity solutions for FACTS and related devices to mitigate risks from cyberattacks directed towards FACTS controllers, stations, and the power grid. The result of the project will be cybersecurity enhanced FACTS controllers via a firmware update.
ABB, Inc.	• Duke Energy • Oak Ridge National Laboratory (ORNL) • University of Illinois Urbana-Champaign	Security Enhancements in IEEE-1547 Environments Integrating DER and Area Power Systems	The project will deliver a reference architecture for secure physical and logical connections to distributed energy resources (DER) and the power grid by extending IEEE 1547 (protocol for interconnecting DER with electric power systems) and a reference implementation to facilitate adoption by the stakeholder community.
Dragos	• Ameren • First Energy • Idaho National Laboratory (INL) • NERC E-ISAC • Southern Company	The Neighborhood Keeper	The project team will develop, and demonstrate a low-cost cloud-enabled sensor network within the operations technology (OT) domain to enable integration of available technologies that will facilitate real-time and actionable information to reduce cyber risk.
GE Global Research	• Baker Hughes • General Electric (GE) • Idaho National Laboratory (INL)	Cyber-Physical Protection for Natural Gas Compression	The project team will develop an advanced cyber-physical protection (CPP) system for natural gas compressor stations through machine learning, advanced control algorithms, and cyber-physical models that monitor key nodes, detect anomalies, and neutralize cyber-attacks.
GE Global Research	• GE Renewable Energy • Idaho National Laboratory (INL)	Cyber-Physical Resilience for Wind Power Generation	The project team will develop adaptive defense technologies for wind power generation systems, using physical models and machine learning techniques that detect, localize and continue operation to survive sophisticated cyber-attacks.
GE Global Research	• Electric Power Board of Chattanooga • MITRE • Oak Ridge National Laboratory (ORNL) • Qubitekk	Time-Sensitive Quantum Key Distribution	The project team will integrate Time-Sensitive Networking (TSN) with Quantum Key Distribution (QKD) to increase availability, strengthen integrity and reveal attempted intrusions in real-time for power grid communications.

Project Performer	Project Partners	Project Title	Project Description
Schweitzer Engineering Laboratories, Inc.	• Bonneville Power Administration (BPA) • Dragos • Juniper Networks	The Ambassador Project	The project team will develop security orchestration for a software defined networking (SDN) flow controller which will provide complete network visibility, situational awareness, automated flows creation, and active defense measures for detected threats in the operational network.
TDi Technologies, Inc.	• EPRI Labs • Exelon • NRG Energy • Oak Ridge National Laboratory (ORNL)	Project Corbomite	The project team will develop a cybersecurity solution that monitors running memory and firmware configurations of embedded devices used in energy delivery control systems to validate integrity so devices can be trusted to operate as expected.
Texas A&M Engineering Experiment Station	• Pacific Northwest National Laboratory (PNNL) • Sandia National Laboratory (SNL) • Sekurity • University of Illinois Urbana-Champaign • Vistra Energy	Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management	The project team will develop a next-generation secure energy management system (EMS) that can detect malicious and abnormal events through fusion of cyber and physical data and algorithms, effective integrated analytics and visualization.
United Technologies Research Center	• Pacific Northwest National Laboratory (PNNL) • Southern California Edison • University of Tennessee Knoxville	WISP: Watching grid Infrastructure Stealthily through Proxies	The project team will develop an open-source tool that uses publicly available metadata, such as real time prices, to detect and alert operators that information has been manipulated with the intent to disrupt energy delivery system operations.
WhiteScope	Multiple energy sector partners	Automated Configuration Analysis Tool for the Oil and Natural Gas Environment	The project team will develop an Automated Configuration Analysis Tool for ONG that provides a secure means to examine device configurations, audit system settings, define security policies, and obtain reporting.